FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 149975]

Privacy Act of 1974; System of Records

AGENCY: Federal Communications Commission.

ACTION: Notice of a modified system of records.

SUMMARY: The Federal Communications Commission (FCC, Commission, or Agency) proposes to modify an existing system of records, FCC/OIG-3, Investigative and Audit Files (formerly: FCC/OIG-3, Investigative Files) subject to the Privacy Act of 1974, as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the *Federal Register* notice of the existence and character of records maintained by the agency. The FCC uses the investigative and audit files contained in the records in this system to carry out its duties and responsibilities under the Inspector General Act of 1978, as amended. This modification changes the scope of this system of records to add new routine uses, to update the exemptions the FCC claims for this system, and to make other changes.

DATES: This modified system of records will become effective on **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written comments on the routine uses are due by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The routine uses will become effective on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, unless written comments are received that require a contrary determination.

ADDRESSES: Send comments to Katherine C. Clark, Federal Communications Commission (FCC), 45 L Street, NE, Washington, DC 20554.

FOR FURTHER INFORMATION CONTACT: Katherine C. Clark, (202) 418-1773, or privacy@fcc.gov (and to obtain a copy of the Narrative Statement and the Supplementary Document, which includes details of the proposed alterations to this system of records).

SUPPLEMENTARY INFORMATION: As required by the Privacy Act of 1974, as amended, 5 U.S.C. 552a(e)(4) and (e)(11), this document sets forth notice of the proposed modification of a system of records maintained by the FCC. This notice modifies a system of records (FCC/OIG-3) maintained by the FCC. The FCC previously provided notice of the system of records FCC/OIG-3, Investigative and Audit Files, by publication in the *Federal Register* on August 26, 2011 (76 FR 53454). The FCC Office of Inspector General (OIG) created this system of records in 2011 by combining into a single system of records the OIG's criminal and civil investigative files and its audit files. OIG uses the records in this system to carry out its duties and responsibilities under the Inspector General Act of 1978, as amended.

The substantive changes and modifications to the previously published version of FCC/OIG-3 include:

1. Renaming this SORN as "Investigative and Audit Files";

2. Modifying the language in the Categories of Individuals and Categories of Records to be consistent with the language and phrasing now used in FCC SORNs;

3. Updating and/or revising language in the following routine uses: Law Enforcement and Investigation, Adjudication and Litigation, Disclosure to the Council of Inspectors General on Integrity and Efficiency (CIGIE), Disclosure for Qualitative Assessment Reviews, and Breach Notification;

4. Adding four new routine uses: (a) Assistance to Federal Agencies and Entities Related to Breaches—to assist with other Federal agencies' data breach situations, which is required by OMB Memorandum No. M-17-12; (b) Non-Federal Personnel—to allow contractors, grantees, and volunteers who have been engaged to assist the

FCC in the performance of a contract service, grant, cooperative agreement with access to information; (c) To provide information to a Congressional member's office from the record of an individual in response to an inquiry from that Congressional office made at the request of that individual; and (d) Congress, congressional committees, or the staffs thereof—to provide Congress, congressional committees and congressional staff access to final FCC-OIG reports or management alerts when the Inspector General (IG) determines that its disclosure is necessary to fulfill the IG's responsibilities under the IG Act of 1978, as amended;

5. Updating the existing records retention and disposal schedule with a new National Archives and Records Administration (NARA) Records Schedule: Office of Inspector General (OIG)—Investigative Files, N1-173-07-002, which was approved by NARA in May 2017;

6. Expanding the scope of the system to expressly include materials related to OIG audits that may contain information about individuals; and

7. Updating the reference to the exemptions claimed under subsections (j) and (k) of the Privacy Act.

The system of records is also updated to reflect various administrative changes related to the system managers and system addresses; policies and practices for storage and retrieval of the information; administrative, technical, and physical safeguards; and updated notification, records access, and contesting records procedures.

SYSTEM NAME AND NUMBER: FCC/OIG-3, Investigative and Audit Files.

SECURITY CLASSIFICATION: Sensitive, but not Classified.

SYSTEM LOCATION: OIG, FCC, 45 L Street, N.E., Washington, DC 20554, and OIG, FCC, 9201 Farm House Lane. Columbia, MD 21046.

SYSTEM MANAGER(S): Johnny Drake, OIG, FCC, 45 L Street, N.E., Washington, DC 20554.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Inspector General Act of 1978, as amended. 5 U.S.C. app.

PURPOSE(S) OF THE SYSTEM: This system will collect, pursuant to the Inspector General Act of 1978:

1. Files and documents for investigations initiated and/or referred by or to the OIG or other investigative agencies regarding FCC programs and operations; and reports regarding the results of investigations to other Federal agencies, other public authorities, or professional organizations that have the authority to bring criminal prosecutions or civil or administrative actions, or to impose other disciplinary sanctions;
2. Files and documents for documenting the outcome of OIG investigations;
3. Records of the activities that were the subject of investigations;
4. Reports, files, and documents for investigative findings to the Commission management about problems and deficiencies in the FCC's programs and operations or to suggest corrective action in reference to identified irregularities, problems, or deficiencies;
5. Records of complaints and allegations received relative to FCC programs and operations and documenting the outcome of OIG reviews of those complaints and allegations;
6. Files and documents for coordinating relationships with other Federal agencies, State and local governmental agencies, and nongovernmental entities in matters relating to the statutory responsibilities of the OIG;
7. Files and documents providing the information necessary to fulfill the reporting requirements of the Inspector General Act of 1978;

8. Files and documents for audits, inspections and evaluations, and surveys conducted by the OIG regarding FCC programs and operations; and

9. Documents for the results of audits, inspections, evaluations and surveys initiated internally or mandated or requested by Congress or other regulatory agencies regarding FCC programs and operations and reporting the results of audits to Congress, Office of Management and Budget (OMB), Government Accountability Office (GAO), and other regulatory and oversight agencies.

Collecting and maintaining these types of information is necessary for key activities discussed in this SORN, including analyzing the effectiveness and efficiency of FCC programs, informing future rulemaking and policymaking activity, and improving staff efficiency.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals who are or have been the subjects of investigations conducted by the OIG;

2. Individuals who are: witnesses, complainants, informants, suspects, defendants, parties identified by the OIG or by other agencies, constituent units of the FCC and members of the general public in connection with the authorized functions of the OIG; and

3. Individuals who provide information during interviews, walkthroughs, questionnaires, demonstrations, and simulations during OIG audits, inspections, and evaluations.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Files developed during investigations of: known or alleged fraud, waste, and abuse; other irregularities; or violations of laws, regulations, orders, or requirements;

2. Files related to programs and operations administered or financed by the FCC, including contractors and others doing business with the FCC;

3. Files relating to FCC employees' hotline complaints and other miscellaneous complaints;

4. Investigative reports and related documents, such as correspondence, notes, attachments, and working papers; and

5. Audit reports and supporting documentation, such as correspondence, memoranda, transcripts, notes, computations, flowcharts, illustrations and summaries.

RECORD SOURCE CATEGORIES:

Under the authority granted to heads of agencies by 5 U.S.C. 552a(j)-(k), the FCC has determined that this system of records is exempt from disclosing the categories of sources of records for this system of records, 47 CFR 0.561.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside of the FCC as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. Law Enforcement and Investigation—Where there is an indication of a violation or potential violation of a statute, regulation, rule, order, or other requirements, records from this system may be shared with appropriate Federal, State, Tribal, or local authorities for purposes of either obtaining additional information relevant to a FCC decision or referring the record for investigation, enforcement, or prosecution by another agency.

2. Disclosure to Public and Private Entities to Obtain Information Relevant to FCC Functions and Duties—The OIG may disclose information from this system to public or private sources to the extent necessary to obtain information from those sources relevant to an OIG investigation, inspection, or audit.

3. Litigation—To disclose records to the Department of Justice (DOJ) when: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the DOJ or the FCC has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation, and the use of such records by the Department of Justice is for a purpose that is compatible with the purpose for which the FCC collected the records.

4. Adjudication—To disclose records in a proceeding before a court or adjudicative body, when: (a) the FCC or any component thereof; or (b) any employee of the FCC in his or her official capacity; or (c) any employee of the FCC in his or her individual capacity; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation, and that the use of such records is for a purpose that is compatible with the purpose for which the agency collected the records.

5. Disclosure to Contractors and Consultants—OIG may disclose a record from this system to the employees of any entity or individual with whom the FCC contracts for the purpose of performing any functions or analyses that facilitate or are relevant to an OIG investigation, audit, inspection, or other inquiry. Before entering into such a contract, the OIG shall require the contractor to maintain Privacy Act safeguards, including as required under the Federal Acquisition Regulations (FAR) Privacy Act provisions (subparts 24.1 and 24.2) and include the specified contract clauses (parts 52.224-1 and 52.224-2), as appropriate, to ensure that personal information by contractors who work on FCC-owned systems of records and the system data are protected as mandated.

6. Debarment and Suspension Disclosure —The OIG may disclose information from this system to the FCC or another Federal agency considering suspension or debarment action if the information is relevant to the suspension or debarment action. The OIG also may disclose information to the FCC or another agency to gain information in support of the FCC's own debarment and suspension actions.

7. Government-Wide Program Management and Oversight—The OIG may disclose a record from this system to the Department of Justice (DOJ) to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or the OMB to obtain that office's advice regarding obligations under the Privacy Act.

8. Prevention of Fraud, Waste, and Abuse Disclosure—The OIG may disclose a record from this system to Federal agencies, non-Federal entities, their employees, and agents (including contractors, their agents or employees; employees or contractors of the agents or designated agents); or contractors, their employees or agents with whom the FCC has a contract, service agreement, cooperative agreement, or computer matching agreement for the purpose of: (1) detection, prevention, and recovery of improper payments; (2) detection and prevention of fraud, waste, and abuse in Federal programs administered by a Federal agency or non-Federal entity; (3) detection of fraud, waste, and abuse by individuals in their operations and programs, but only to the extent that the information shared is necessary and relevant to verify pre-award and prepayment requirements prior to the release of Federal funds, prevent and recover improper payments for services rendered under programs of the FCC or of those Federal agencies and non-Federal entities to which the FCC provides information under this routine use.

9. Disclosure to CIGIE —The OIG may disclose a record from this system to members and employees of CIGIE for the preparation of reports to the President and Congress on the activities of the Inspectors General.

10. Disclosure for Qualitative Assessment Reviews—The OIG may disclose a record from this system to members of CIGIE, the DOJ, the U.S. Marshals Service, or any Federal agency for the purpose of conducting qualitative assessment reviews of the investigative operations of the OIG to ensure that adequate internal safeguards and management procedures are maintained.

11. Breach Notification—To appropriate agencies, entities, and persons when: (a) the Commission suspects or has confirmed that there has been a breach of PII maintained in the system of records; (b) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

12. Assistance to Federal Agencies and Entities Related to Breaches—To another Federal agency or Federal entity, when the Commission determines that information from this system is reasonably necessary to assist the recipient agency or entity in: (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, program, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

13. Non-Federal Personnel—To disclose information to non-Federal personnel, including contractors, grantees, and volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related

to this system of records and who need to have access to the records in order to perform their activity.

14. To provide information to a Congressional member's office from the record of an individual in response to an inquiry from that Congressional office made at the request of that individual.

15. To Congress, congressional committees, or the staffs thereof once an FCC-OIG report or management alert has become final and the IG determines that its disclosure is necessary to fulfill the IG's responsibilities under the IG Act of 1978, as amended.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Information in this system consists of paper records, documents, and files in file folders and electronic records, files, and data that are stored in the OIG databases that are part of the FCC's computer network. Electronic records may also be contained in databases that are not part of FCC's computer network, and also are stored in removable drives, computers, and other electronic databases.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records in this system of records can be retrieved by any category field, e.g., first name or email address, or by a unique file number assigned to each matter.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The information in this system is maintained and disposed of in accordance with the National Archives and Records Administration (NARA) Records Schedule: Office of Inspector General (OIG)—Investigative Files, N1-173-07-002, Item 1.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The paper, diskette, and records contained in other media are password protected or kept in locked storage that is further secured at the end of each business day. Limited access to these records is permitted by those persons whose official duties require such access; thus, unauthorized examination during business hours would be easily detected.

The electronic records, files, and data are maintained in the FCC computer network databases. Access to the electronic files is restricted to authorized OIG supervisors and staff. Authorized OIG staff and OIG contractors and authorized staff and contractors in the FCC's Information Technology Center (ITC) have access to the electronic files on an "as needed" basis. Backup media are stored on-site and at a secured, off-site location. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features to prevent unauthorized users from gaining access to the data and system resources. This comprehensive and dynamic set of IT safety and security protocols and features is designed to meet all Federal privacy standards, including those required by the Federal Information Security Modernization Act of 2014 (FISMA), OMB, and the National Institute of Standards and Technology (NIST).

RECORD ACCESS PROCEDURES: Under the authority granted to heads of agencies by 5 U.S.C. 552a(j)-(k), the FCC has determined that this system of records is exempt from disclosing its record access procedures for this system of records, 47 CFR 0.561.

CONTESTING RECORD PROCEDURES: Under the authority granted to heads of agencies by 5 U.S.C. 552a(j)-(k), the FCC has determined that this system of records is exempt from disclosing its contesting record procedures for this system of records, 47 CFR 0.561.

NOTIFICATION PROCEDURES: Under the authority granted to heads of agencies by 5 U.S.C. 552a(j)-(k), the FCC has determined that this system of records is exempt from the notification procedure for this system of records. 47 CFR 0.561.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to subsection 0.561 of the Commission's rules, 47 CFR 0.561, this system of records is exempt from §§ (c)(3), (c)(4), (d), (e)(1) through(3), (e)(4)(G) through(I), (e)(5), (e)(8), (f), and (g) of the Privacy Act and from 47 CFR 0.554–0.557 of the Commission's rules. These provisions concern individuals' rights to access and amend information about themselves, and an agency's duties to provide notice about

how individuals can access information about themselves. The system is exempt from these provisions because it contains the types of materials described in subsections (j)(2) and (k)(1)-(2) of the Privacy Act.

HISTORY: The FCC created this system of records (OIG-3) in 2011 by combining into a single system of records the OIG's criminal and civil investigative files, 76 Fed. Reg. 53454 (Aug. 26, 2011).

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2023-13512 Filed: 6/23/2023 8:45 am; Publication Date: 6/26/2023]